Ebook

Comment mettre en place un SOC ?

SiGMA
NUMÉRIQUE À IMPACT

47 % des entreprises déclarent avoir subi au moins une cyberattaque réussie en 2024,

un chiffre qui n'évolue pas par rapport à l'année précédente, mais qui témoigne toujours de l'intensité de la menace (Baromètre CESIN 2025).

Celles-ci ont entraîné des pertes financières s'élevant en moyenne à 14 720 euros, et dépassant 230 000 euros dans un cas sur huit.

Mais ces chiffres alarmants ne sont que la partie visible de l'iceberg. Au-delà des pertes financières, les conséquences d'une cyberattaque sont souvent d'une plus grande ampleur : interruption d'activité, atteinte à la réputation, perte de données critiques et, dans les cas les plus graves, faillite de l'entreprise.

Les TPE/PME et ETI sont particulièrement exposées. Disposant de ressources limitées et souvent moins bien outillées pour faire face à des incidents de sécurité sophistiqués, elles constituent des cibles privilégiées pour les acteurs malveillants. Les chiffres du rapport Hiscox sont éloquents : le nombre de PME de moins de dix salariés victimes d'une cyberattaque a été multiplié par deux au cours des trois dernières années. Cette tendance inquiétante souligne l'urgence d'agir.

Cependant, aucune organisation n'est épargnée, quelle que soit sa taille, quel que soit son secteur. Alors que le risque de défaillance est multiplié par deux dans les six mois suivant une cyberattaque, la mise en place d'une stratégie de cybersécurité robuste et proactive n'est plus une option, mais une nécessité.

Au cœur de cette stratégie de sécurité se trouve le SOC (Security Operations Center). Véritable tour de contrôle de la sécurité informatique, il assure une surveillance continue, une détection précoce et une réponse rapide aux cybermenaces, 24 heures sur 24 et 7 jours sur 7.

Cependant, lorsque l'entreprise envisage la mise en place d'un SOC, les questions sont nombreuses : comment mettre en place un SOC véritablement efficace ? Quelles options s'offrent aux organisations ? Quelles ressources technologiques et humaines sont nécessaires ?

Cet ebook apporte des réponses concrètes et pragmatiques, adaptées à la réalité du terrain et aux contraintes des entreprises. Il vous guidera pas à pas dans la construction d'une défense cybersécurité à la hauteur des menaces actuelles.

SOMMAIRE

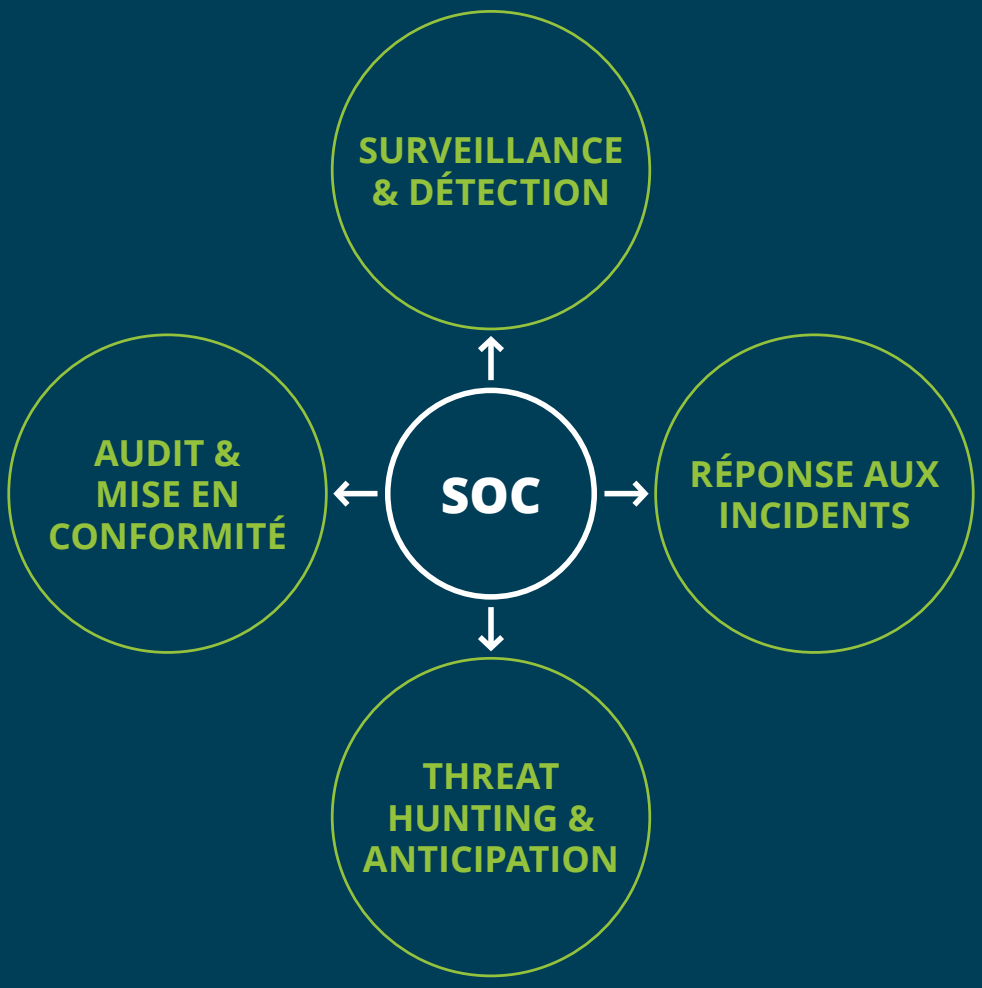
LE SOC : VOTRE BOUCLIER FACE AUX CYBERMENACES

Qu'est-ce qu'un SOC ?

Imaginez un centre de commandement ou une unité centralisée qui audite et surveille la sécurité de votre système d'information (SI) 24h/24 et 7j/7. Composé d'experts en sécurité, d'analystes et d'ingénieurs équipés d'outils et de solutions de pointe : SIEM (Security Information and Event Management), EDR (Endpoint Detection and Response), XDR (Extended Detection and Response), SOAR (Security Orchestration, Automation and Response), cette unité centralisée peut prendre la forme d'une équipe interne, d'un service externalisé ou d'une combinaison des deux.

Le SOC, véritable tour de contrôle de votre cybersécurité, agit comme un système nerveux central qui collecte, analyse et traite en temps réel l'ensemble des informations de sécurité de votre système d'information. Votre entreprise bénéficie ainsi d'une meilleure maîtrise de son environnement de sécurité et peut prendre des décisions éclairées pour se protéger.

Les missions essentielles du SOC



SURVEILLANCE CONTINUE & DÉTECTION 24H/24

Le SOC opère comme un centre de commande dans lequel des professionnels de la cybersécurité assurent une surveillance permanente de votre système d'information, 24h/24, 7j/7 et 365 jours par an, selon vos besoins opérationnels. Grâce à ses outils d'analyse avancée, le SOC peut détecter les comportements suspects et les anomalies avant qu'ils ne se transforment en incidents majeurs.

RÉPONSE AUX INCIDENTS

Lorsque le SOC détecte une intrusion, chaque seconde compte. Les experts en cybersécurité le composant déploient immédiatement un protocole d'intervention destiné à bloquer et éradiquer la menace.

En cas de cyberattaque, ils s'attachent à la circonscrire et à mettre en place le plan de continuité ou le plan de reprise (PCA et PRA) qui préservera votre activité.

APPRENTISSAGE & ANTICIPATION

La meilleure défense face aux attaques, c'est l'anticipation. Le SOC ne se contente pas d'attendre les menaces, il les traque activement. Cette démarche proactive, le « threat hunting », permet d'identifier et de neutraliser les risques avant qu'ils ne se concrétisent.

Parallèlement, le SOC applique une stratégie de maintenance orientée risque en identifiant et en corrigeant les vulnérabilités, en prévenant et en améliorant les outils et les pratiques.

RESPECT DE LA RÉGLEMENTATION

Outre la perte financière due à l'interruption de l'activité et au coût des réparations, une cyberattaque entraîne un risque de sanctions légales et financières en cas de défaut de conformité aux réglementations de protections des données : directive NIS2, RGPD, PCI DSS...

Tout en assurant une protection optimale de votre SI, le SOC veille au respect des différentes réglementations.

Pour remplir sa mission, il assure, par exemple, la journalisation des événements, la traçabilité des accès et la mise en place de procédures de sécurité dans le strict respect de la directive NIS2.

Le saviez-vous ?

Après une cyberattaque, le retour à un niveau normal d'activité nécessite en moyenne respectivement 26 et 29 jours pour les TPE et les PME.

Pourquoi le SOC est-il devenu indispensable pour les entreprises ?

L'émergence des SOC n'est pas le fruit du hasard, mais une réponse nécessaire à la transformation du paysage numérique. Les cybermenaces sont de plus en plus complexes et fréquentes. Les acteurs malveillants ont évolué, passant d'individus isolés à des entités hautement structurées disposant d'infrastructures techniques comparables à celles d'organisations légitimes. Les attaques ne ciblent plus seulement les grandes entreprises, mais balaient désormais tous les secteurs et toutes les organisations sans distinction de taille ou de domaine d'activité.

Parallèlement, la transformation numérique et l'évolution des modes de travail ont considérablement élargi les surfaces d'attaques. Le développement du recours aux clouds (interne ou externe), le travail à distance, la multiplication des objets connectés et l'interconnexion croissante des systèmes ont mécaniquement augmenté les vulnérabilités.

Les technologies d'intelligence artificielle générative constituent aujourd'hui un vecteur de risque critique pour la préservation des actifs intellectuels des entreprises. Selon les analyses prospectives du cabinet Gartner, les problématiques liées à l'IA générative représentent désormais le second facteur de préoccupation des RSSI, directement derrière les vulnérabilités liées aux services tiers. Ces outils peuvent involontairement exposer des données sensibles (informations stratégiques, code source, données financières…) dans les environnements cloud.

Les réglementations ont de leur côté durci le cadre juridique de la protection des données. Ainsi, le Règlement Général sur la Protection des Données (RGPD) impose des obligations strictes en matière de sécurisation des données personnelles. Les sanctions financières peuvent atteindre 4 % du chiffre d'affaires mondial ou 20 millions d'euros (article 83 du RGPD) créant une pression réglementaire sans précédent sur les directions informatiques.

Dans ce contexte, la veille technologique s'impose comme un impératif. Les techniques des cybercriminels évoluent à une vitesse exponentielle. Les nouveaux vecteurs d'attaques comme les attaques d'ingénierie sociale tel le phishing ou les menaces persistantes avancées (APT) nécessitent une vigilance et des compétences en perpétuelle évolution.

À ce titre, l'intelligence artificielle se caractérise par son ambivalence, constituant simultanément un levier d'optimisation et une menace pour l'écosystème de la cybersécurité.

Si elle offre des capacités inédites de détection et de prévention des cyberattaques (analyse prédictive des menaces, détection en temps réel des anomalies, réponses automatisées aux attaques), elle devient également un terrain de jeu dangereux où les cybercriminels développent des attaques de plus en plus sophistiquées, capables de contourner les systèmes de défense traditionnels, d'exploiter des vulnérabilités inédites et de mimer des comportements humains avec une précision déconcertante.

La continuité opérationnelle, la préservation de la réputation, la protection des données clients et la sécurisation des actifs constituent des impératifs incontournables. La mise en place d'un SOC permet alors de transformer la contrainte « cybersécurité » en un avantage concurrentiel.

Pour l'entreprise, les dirigeants et les RSI, disposer d'un SOC devient également un élément de différenciation. C'est la démonstration d'un engagement concret sur la voie de la sécurité, un signal fort adressé aux clients, aux partenaires et aux investisseurs.

Dans ce contexte multidimensionnel, le SOC représente la seule réponse véritablement proactive et adaptative pour répondre à des cybermenaces qui se caractérisent par une complexité et une sophistication croissantes.

COMMENT METTRE EN PLACE UN SOC POUR SON ENTREPRISE ?

La création et le déploiement d'un Security Operations Center représentent un processus stratégique complexe qui nécessite une approche méthodologique rigoureuse. Chaque étape doit être pensée avec précision pour garantir, à la fin, l'efficacité du dispositif.

1

Étape 1 :
définir les objectifs et le périmètre de votre SOC

↓

2

Étape 2 :
constituer l'équipe du SOC

↓

3

Étape 3 :
Choix des technologies et des outils

↓

4

Étape 4 :
Développement des processus et procédures

↓

5

Étape 5 :
Mise en œuvre et intégration

Étape 1 :
définir les objectifs et le périmètre de votre SOC

Avant de déployer un SOC, il est indispensable de réaliser un état des lieux et une évaluation des besoins. Cette phase permet de déterminer la stratégie et les objectifs de sécurité adaptée à l'entreprise.

Pour vous aider dans cette démarche, un audit de maturité, tel que celui proposé par Sigma s'avère un outil précieux. Se basant sur 8 piliers et 60 critères, il offre une vision claire de la situation actuelle en matière de sécurité des données, de gouvernance et d'infrastructures. Il comprend des évaluations approfondies, notamment un diagnostic d'exposition web, un audit Active Directory et un scan de vulnérabilité, permettant de prendre des décisions stratégiques et de se focaliser sur les priorités.

Fort de cette évaluation approfondie, vous serez en mesure de définir avec précision la portée de votre SOC. Cette étape est cruciale, car elle détermine les activités du SOC et guide l'élaboration de politiques et procédures pertinentes. La sécurité est souvent perçue comme entrant en conflit avec d'autres actions au sein de l'entreprise. Aligner la stratégie du SOC sur les objectifs de performances peut agir de façon à ce que la sécurité soit considérée comme un atout et un élément essentiel du succès de votre organisation.

Exemples d'objectifs SMART :

- Réduire le temps moyen de détection des incidents de sécurité de X % d'ici [date].
- Atteindre un taux de conformité RGPD de 100 %.
- Diminuer le nombre d'incidents de sécurité majeur de X % par an.

La formulation des objectifs du SOC nécessite également une cartographie complète de votre système d'information. Cet audit implique d'identifier les actifs numériques, en particulier les actifs critiques (données sensibles, applications...).

Enfin, il est nécessaire de se poser quelques questions :

- Quels sont les processus critiques et leur donnée qui font l'existence de l'entreprise sur son marché ?
- Quel est le profil de risque de l'entreprise ?
- Quelles sont les contraintes budgétaires ?
- Quel est l'environnement technique de l'organisation ? (Infrastructure réseau, services cloud, terminaux...)

En prenant en compte les besoins spécifiques de votre entreprise en matière de sécurité, vous adapterez votre SOC pour qu'il y réponde de manière efficace. Sigma peut vous aider à faire le point.

Étape 2 : constituer l'équipe du SOC

L'efficacité d'un SOC repose en grande partie sur l'équipe qui le compose. Chaque membre apporte son expertise, formant un ensemble capable de détecter, analyser, neutraliser des menaces sophistiquées, mais également capable de former et sensibiliser les collaborateurs à la cybersécurité.

Pour constituer l'équipe, il est nécessaire de déterminer quelle expertise est indispensable en fonction de la taille et des besoins de l'organisation. Se trouvent généralement au sein d'un SOC :

- Des analystes de sécurité ou analystes SOC : chargés de surveiller les alertes, d'enquêter sur les menaces et de répondre aux incidents ;
- Un responsable SOC ou responsable SSI (Sécurité des Systèmes d'Information) qui supervise les opérations du SOC, gère le personnel, coordonne la réponse aux incidents et surveille les performances ;
- Des ingénieurs ou des architectes cybersécurité : chargés de concevoir, mettre en œuvre, administrer et maintenir les architectures matérielles et logicielles du SOC, d'assurer l'assistance technique, de mettre au point la documentation des processus ou encore de faire appliquer les éléments de la politique de sécurité.

Au-delà des compétences techniques, la culture de la cybersécurité est le ciment de cette équipe SOC. Cependant, des processus clairs, des protocoles bien définis et une communication fluide sont essentiels pour que cette unité soit réellement performante.

Là aussi, des questions sont à se poser :

- Quelles sont les compétences déjà présentes en interne ?
- Faut-il recruter de nouveaux experts ou miser sur la formation ?
- Quel budget allouer à cette évolution organisationnelle et son maintien en compétence ?

Le saviez-vous ? Il manque plus de 4 millions d'experts en cybersécurité dans le monde (source : ISC2). La DGSE estime quant à elle que 15 000 experts seraient nécessaires pour répondre au besoin en cybersécurité des entreprises françaises.

Étape 3 : choisir les bons outils et les technologies

La performance du SOC repose sur sa capacité à intégrer des solutions technologiques de pointe sans toutefois accumuler les outils. Il s'agit de créer un écosystème numérique intelligent et réactif. Parce qu'elles capturent et analysent en temps réel les flux d'information, les solutions de monitoring représentent le premier rempart de votre système.

Le SIEM est le cerveau du SOC. Il centralise et relie les événements et toutes les informations de sécurité. Il transforme ces données brutes en informations permettant de détecter des comportements anormaux qui auraient pu échapper au regard des experts en cybersécurité. Le SIEM est généralement complété de système de détection d'intrusion.

Les outils d'analyse et de réponse apportent quant à eux une dimension dynamique à la cyberdéfense. Les solutions EDR aident à détecter et répondre aux menaces. Les plateformes XDR étendent cette protection en intégrant des données provenant de multiples sources alors que les technologies SOAR permettent d'automatiser les réponses aux incidents, réduisant ainsi les temps de réaction.

Le choix des outils et des technologies est un investissement stratégique : ceux-ci doivent permettre d'anticiper les menaces de demain tout en s'adaptant aux spécificités de votre entreprise.

Étape 4 : développer des processus et des procédures

Les processus mis en place au sein du SOC doivent couvrir tous les aspects des opérations de sécurité : de la détection des menaces à la réponse aux incidents. Tous les processus doivent être rigoureusement documentés.

Pour cela, il est nécessaire de :

- Définir un plan de réponse aux incidents avec les mesures à prendre en cas d'incident de sécurité, y compris les rôles et les responsabilités.
- Mettre en place des règles et des alertes pour identifier les menaces.
- Intégrer le renseignement sur les menaces aux activités de surveillance et de réponse.
- Développer un système de signalement des incidents et de mesure de l'efficacité du SOC (rapports réguliers, indicateurs clés de performance [KPI]...
- Identifier les menaces qui pèsent sur l'entreprise et déterminer comment le SOC peut les détecter et les bloquer.

Les processus et procédures doivent être régulièrement interrogés. Chaque crise surmontée, chaque menace neutralisée, chaque vulnérabilité détectée devient une opportunité d'apprentissage, permettant de renforcer la résilience de l'entreprise.

Étape 5 : Déployer et faire vivre le SOC - démarche d'amélioration continue

Une fois ses objectifs définis, son équipe constituée, et les outils et les processus définis, il est temps de mettre en place votre SOC. Cette étape implique de déployer le matériel et les technologies nécessaires, de commencer à collecter les données et de s'assurer que tous les outils et systèmes sont correctement intégrés.

Mais un SOC n'est pas une solution statique. Il doit être capable de s'adapter constamment face aux menaces émergentes. Son équipe doit analyser méticuleusement les stratégies utilisées dans les cyberattaques, les points de pénétration, les réactions mises en place. Cette approche rétrospective nourrit directement le système, affinant les algorithmes de détection et les protocoles de réponses.

Le SOC est amené à évoluer. La veille technologique permet aux professionnels du SOC de scruter en permanence l'horizon numérique et d'anticiper les nouvelles menaces, les failles émergentes, les technologies de défense innovantes. Cette vigilance constante du SOC permet de maintenir une longueur d'avance sur les acteurs malveillants.

SOC INTERNALISÉ OU SOC EXTERNALISÉ : COMMENT CHOISIR ?

Un SOC interne est une unité de cybersécurité centralisée entièrement détenue et gérée par l'entreprise alors qu'un SOC externe est un service fourni par un prestataire spécialisé qui prend en charge la surveillance, la détection et la réponse aux incidents pour le compte de l'entreprise cliente.

Internaliser son SOC, une solution exigeante pour une maîtrise totale de sa sécurité

PERSONNALISATION & MAÎTRISE DE SA CYBERSÉCURITÉ

Le choix du SOC internalisé peut sembler séduisant au premier abord. L'attrait de la maîtrise totale et du contrôle direct des opérations de sécurité est en effet indéniable. L'adaptation du SOC aux problématiques et aux besoins de l'entreprise peut également paraître plus facile et plus rapide à réaliser avec une équipe déjà présente en interne.

RISQUES DE COÛTS CACHÉS

Cependant, la réalité peut rapidement révéler une complexité opérationnelle et financière souvent sous-estimée par les décideurs.

En effet, le coût réel d'un SOC interne dépasse largement les simples investissements technologiques. Il implique un engagement humain et financier souvent considérable. Les entreprises doivent recruter des professionnels hautement qualifiés sur un marché de la cybersécurité extrêmement concurrentiel. Ces experts, rares et très recherchés, exigent des rémunérations attractives qui peuvent rapidement grever votre budget IT.

BESOIN EN RESSOURCES ET COMPÉTENCES

La maintenance d'un SOC interne implique également un investissement permanent en formation et en veille technologique. Les technologies de cybersécurité évoluent à une vitesse vertigineuse. Chaque nouvelle menace, chaque nouvelle technique d'attaque, imposent également une mise à jour constante des compétences et des outils. Pour une entreprise, suivre ce rythme représente souvent un défi considérable en termes de ressources, mais également de compétences.

DÉFIS ORGANISATIONNELS

Au-delà de l'aspect financier, l'internalisation du SOC pose des défis organisationnels majeurs. La cybersécurité ne connaît pas de pause : les menaces évoluent 24 heures sur 24, 7 jours sur 7 et 365 jours par an. Les équipes SOC font face à une pression constante et doivent faire preuve d'une vigilance de tous les instants. Ces rythmes peuvent rapidement conduire à un épuisement des experts et créer un turn-over déstabilisant pour la sécurité de votre SI.

Externaliser son SOC, l'option de la souplesse et de la réactivité

Au vu de ces contraintes, l'externalisation du SOC représente une alternative particulièrement attractive pour les entreprises qui recherchent efficacité et optimisation des coûts.

EXPERTISE IMMÉDIATE ET MUTUALISÉE

En effet, le principal avantage d'un SOC externe réside dans l'accès immédiat à une expertise de haut niveau sans les nécessités de recrutement et le coût d'une équipe interne. Les prestataires spécialisés possèdent des équipes de cybersécurités rompues aux dernières techniques de détection et de réponse aux incidents et constamment formées aux évolutions des menaces.

FLEXIBILITÉ ET ADAPTABILITÉ (SCALABILITÉ)

La flexibilité constitue un autre atout déterminant. Un SOC externalisé s'adapte instantanément aux besoins changeants de l'entreprise. Qu'il s'agisse de monter en puissance face à une menace émergente ou de redimensionner le dispositif selon la croissance de l'organisation, le prestataire absorbe ces variations sans contrainte opérationnelle pour le client.

DISPONIBILITÉ CONTINUE

La disponibilité opérationnelle représente également un élément clé. Ces SOC externalisés offrent une surveillance continue, 24 heures sur 24, 7 jours sur 7 et 365 jours par an, comme chez Sigma, éliminant les limitations des équipes internes traditionnelles. Cette veille permanente permet une détection et une réaction rapides aux incidents de sécurité.

MAÎTRISE ET PRÉDICTIBILITÉ DES COÛTS

La mutualisation des ressources permet également de bénéficier d'infrastructures technologiques de pointe à des coûts maîtrisés. Des outils de supervision avancés, des systèmes de corrélation d'événements et des capacités de threat hunting deviennent accessibles avec des investissements moins lourds. Enfin, basées la plupart du temps sur des modèles SAAS, ces technologies ont l'avantage de proposer des modèles économiques à l'asset, plus facilement prévisibles dans votre exercice budgétaire.

CONFORMITÉ ET RECENTRAGE DES ÉQUIPES INTERNES SUR LES PROJETS À VALEUR AJOUTÉE

La dimension réglementaire trouve également une réponse adaptée. Les prestataires garantissent une conformité aux normes de sécurité les plus exigeantes, produisant une documentation précise et une traçabilité exhaustive des incidents.

Enfin, l'externalisation libère les équipes internes des tâches de surveillance continue.
Les ressources informatiques peuvent se recentrer sur des projets à valeur ajoutée, sur l'innovation et le développement stratégique, plutôt que sur la gestion quotidien ne des alertes de sécurité.

	SOC INTERNE	SOC EXTERNE
	Contrôle total et maîtrise des opérations de sécurité	*Partiel*
COÛT	Élevé : recrutement, salaire, formation, infrastructure	Maîtrisé et prévisible : mutualisation des moyens, facturation à l'asset
EXPERTISE	Dépendante des recrutements et de la formation	Accès immédiat à une expertise de pointe et des équipes spécialisées constamment formées
DISPONIBILITÉ	Limitée aux heures de travail ou travail décalé/astreinte	Continue 24/7/365
FLEXBILITÉ	Adapté aux besoins de l'entreprise, mais potentiellement moins flexible face aux changements	Très flexible, s'adapte immédiatement aux besoins changeants (montée en puissance face à une menace, redimensionnement...)
CONFORMITÉ	Nécessite un investissement permanent en formation et veille technologique	Doit être garantie par le prestataire
TECHNOLOGIES	Dépendantes de l'investissement	SIEM, SOAR, XDR, plateformes de threat intelligence...
RÉPONSE AUX INCIDENTS	Peut être limitée par les ressources internes et la disponibilité du personnel	Expertise spécialisée et processus rationalisés pour une réponse rapide et efficace

LE CHOIX STRATÉGIQUE : UN SOC EXTERNE IMPLANTÉ EN FRANCE AVEC SIGMA

Le choix entre internalisation et externalisation du SOC ne relève donc pas d'une simple équation technique, mais d'une stratégie globale qui doit s'aligner avec les objectifs de l'entreprise.

Fort de son expertise et opérant à Nantes et Strasbourg, Sigma propose une solution SOC managée qui se distingue par une disponibilité opérationnelle totale : présence physique sur l'ensemble du territoire national, équipe dédiée et joignable 24h/24, 7j/7, 365j/an, et réactivité immédiate en cas d'incident.

Le SOC Sigma offre la possibilité aux entreprises de bénéficier d'une expertise de haut niveau sans les contraintes d'investissements. Les clients accèdent à des compétences en cybersécurité habituellement réservées aux grands groupes avec une flexibilité et une agilité remarquable.

La proximité géographique constitue également un atout par rapport aux solutions internationales standardisées. Grâce à son implantation nationale, Sigma comprend les spécificités du tissu économique français, les réglementations nationales et les enjeux sectoriels spécifiques.

Un accompagnement personnalisé vient compléter cette offre technique. Chacun de nos clients bénéficie en effet d'un parcours sur-mesure, d'une analyse approfondie de ses besoins et d'une stratégie de sécurité évolutive.

Le SOC Sigma s'appuie sur des technologies leaders de leur marché : Microsoft, Crowdstrike, IBM, Darktrace et des éditeurs français pour apporter des réponses concrètes à vos enjeux de souveraineté

En choisissant Sigma, vous ne souscrivez pas simplement un service SOC, nous établissons avec vous un véritable partenariat stratégique en cybersécurité.

À PROPOS DE SIGMA

Depuis plus de 50 ans, Sigma s'engage pour un numérique responsable et créateur de valeur durable. Nous militons pour un numérique à impact, visant à produire des services numériques utiles à chacun et chacune et respectueux du vivant.

Sigma est spécialisé dans :

- **La cybersécurité et la valorisation des données ;**
- **L'externalisation de systèmes d'information et les solutions cloud ;**
- **L'édition et l'intégration de logiciels et de solutions sur mesure.**

Nous construisons avec vous des solutions qui révèlent les potentiels de vos écosystèmes informatiques.

+ 50 % **Plus de 50 % de nos solutions éco-conçues d'ici 2026 ;**

- 40 % **Réduction de 40 % de nos gaz à effet de serre.**

SiGMA
NUMÉRIQUE À IMPACT

La Gesvrine - 8 rue Newton
La Chapelle-sur-Erdre
Tel. : +33 (0)2 40 37 14 00
https://www.sigma.fr
@groupesigma

Nantes
Paris
Lyon
Toulouse
Strasbourg

700 collaborateurs sur 5 implantations nationales

10 partenaires technologiques majeurs

2200 clients

75 M€ de CA

5 piliers numériques majeurs

- Édition et intégration
- Solutions sur-mesure
- Data valorisation
- Infogérance et Cloud services
- Cybersécurité

Document non contractuel - Sigma Informatique - Siège social : 8 rue Newton CS 84533 - 44200 La Chapelle-sur-Erdre - S.A.S au capital de 1 729 600€ - RCS Nantes B 872 803 390 Siret 872 803 390 00030 - N° TVA intracommunautaire FR39 872 803 390 - APE 6202